## AMENDMENTS TO THE CLAIMS

**Claim 1 (Currently Amended)** A method of uniforming physical random numbers, comprising the steps of: inputting a plurality of physical random numbers to a random number holding device ~~(200)~~ to hold the physical random numbers; ~~them, employing~~ inputting a part of the physical random numbers held in ~~said~~ the random number holding device into addresses ~~as an address of~~ a selector~~, and~~; and randomly selecting and outputting, from the selector, a residual part of the physical random numbers ~~from the residual part~~, based on ~~said address~~ an address value of the part of the physical numbers input into the addresses of the selector.

**Claim 2 (Cancelled)**

**Claim 3 (Currently Amended)** The method of uniforming physical random numbers according to claim 1, further comprising: inputting the output of the selector and a physical random number to ~~wherein~~ an exclusive OR circuit ~~that inputs the output of said selector and the physical random number is provided,~~; and outputting an output of the exclusive OR circuit ~~its output being input~~ into the random number holding device, as a physical random number input into the random number holding device ~~(200)~~.

**Claim 4 (Currently Amended)** A method of uniforming physical random numbers, the method comprising uniforming physical random numbers at multiple stages by repeating the method of ~~operation according to~~ claim 1 for two or more cycles.

**Claim 5 (Currently Amended)** The method of uniforming physical random numbers according to claim 1, wherein the random number holding device is a shift register ~~(200) is employed as the random number holding device~~.

**Claim 6 (Currently Amended)** A physical random number generation device ~~having~~ comprising a physical random number generator, ~~said~~ the physical random number generator comprising:

a serial physical random number generator for generating a serial random number in accordance with a reference clock signal;

a serial/parallel converter for converting the serial random number to a parallel random number;

a plurality of registers capable of ~~holding~~ storing the parallel random number; and

a control circuit for (i) sequentially ~~holding~~ storing the parallel random number in ~~said~~ the plurality of registers ~~every~~ each time the parallel random number is generated by ~~said~~ the serial/parallel converter, ~~and~~ (ii) reading and outputting the parallel random number from ~~said~~ the plurality of registers ~~register~~ in accordance with a read clock signal, and (iii) ~~as well as~~ successively updating ~~the~~ contents of ~~said~~ the plurality of registers by shifting the stored parallel random number from ~~the other~~ a register of the plurality of registers to ~~the~~ another register of the plurality of registers, the other register being a register for which the reading of the parallel random number ~~is~~ has completed ~~ended~~.

**Claim 7 (Currently Amended)** The physical random number generation device according

to claim 6, wherein ~~said~~ the physical random number generator comprises:

an up/down counter for ~~deciding~~ determining, from among the plurality of registers, a register to hold the parallel random number ~~among the plurality of registers~~ and outputting a write address[[,]]; and

a selector for selecting the register to hold the parallel random number, the selection being made based on the write address output by ~~said~~ the up/down counter, and the selector being for outputting ~~to output~~ a load signal based on the selection, ~~and~~

wherein the ~~a~~ control circuit ~~for~~ sequentially stores ~~holding~~ the parallel random numbers in ~~said~~ the serial/parallel converter from ~~the~~ a latter stage register to ~~the~~ a former stage register, from among ~~said~~ the plurality of registers, based on the load signal output from ~~said~~ the selector, ~~and reading and outputting~~ reads and outputs the parallel random number from ~~said~~ a last stage register, from among ~~said~~ the plurality of registers, in accordance with ~~a~~ the read clock signal, ~~and as well as~~ sequentially shifts ~~shifting~~ the parallel random number within ~~each register residing at~~ the former stage ~~of said~~ register to the latter stage register.

**Claim 8 (Currently Amended)** The physical random number generation device according to claim 6, wherein ~~said~~ the physical random number generator comprises (i) a total counter for counting ~~the~~ a total number of serial random numbers generated by ~~said~~ the serial physical random number generator, and (ii) a random number verification circuit for verifying ~~the~~ a uniformity of random numbers, based on the serial random numbers, when the total number of serial random numbers counted by ~~said~~ the total counter reaches a predetermined bit number.

**Claim 9 (Currently Amended)** The physical random number generation device according to claim 8, wherein a random number verification method ~~for said~~ of using the random number verification circuit comprises verifying the uniformity of random numbers by counting ~~the~~ an appearance frequency of a random number value "0" or "1" and comparing ~~it~~ the counted appearance frequency with a prescribed value.

**Claim 10 (Currently Amended)** The physical random number generation device according to claim 8, wherein a random number verification method ~~for said~~ for using the random number verification circuit comprises verifying the uniformity of random numbers by comparing a $\chi$ square value calculated based on ~~the~~ an appearance frequency of each random number value with a prescribed value, ~~with~~ wherein one random number value ~~being~~ is 4 bits.

**Claim 11 (Currently Amended)** The physical random number generation device according to claim 8, wherein ~~the~~ a random number verification method for using the ~~said~~ random number verification circuit comprises verifying the uniformity of random numbers by counting ~~the~~ an appearance frequency of a string for every length of string and comparing ~~it~~ each counted appearance frequency with a prescribed value.

**Claim 12 (Currently Amended)** The physical random number generation device according to claim 8, wherein ~~the~~ a random number verification method for using the ~~said~~ random number verification circuit comprises verifying the uniformity of random numbers by comparing ~~the~~ a length of ~~the~~ a longest string appearing in the random numbers of certain bits with a prescribed

value.

**Claim 13 (Cancelled)**

**Claim 14 (Currently Amended)** The physical random number generation device according to claim 6, further comprising a plurality of physical random number generators, wherein a first~~in which one~~ physical random number generator is selected, from among ~~said~~ the plurality of physical random number generators, based on a select signal of ~~said~~ the selector, to output the random number or random number verification data.

**Claim 15 (Currently Amended)** A physical random number generator comprising:

two integration circuits, each integration circuit for integrating a clock signal through a resistor and a capacitor to output ~~an~~ a respective integral waveform[[,]];

two noise sources[[,]];

two amplifiers, each amplifier for amplifying ~~the~~ a noise ~~of said~~ from a respective noise source of the two noise sources, ~~source~~ to output a respective noise signal[[,]];

two mixers, each mixer for mixing ~~said~~ a respective integral waveform and ~~said~~ a respective noise signal~~, and~~;

two edge detection circuits, each edge detection circuit for detecting ~~the~~ a first edge of jitter generated based on an output waveform of ~~said~~ a respective mixer of the two mixers;

a flip-flop for outputting "0" or "1" based on a phase difference ~~in~~ between respective output signals output from the two ~~the output signal between said~~ edge detection circuits;

a phase adjuster for adjusting ~~the~~ a phase of an input signal input into ~~said~~ each integration circuit, ~~said~~ the phase adjuster including ~~having~~ a delay, a first selector and an up/down counter; and

a feedback circuit for feeding back the output of ~~said~~ the flip-flop to ~~said~~ the phase adjuster so that the "0" or the "1" output from ~~said~~ the flip-flop ~~may converge~~ converges to 50%;

wherein a second selector and a third selector are provided at a ~~the~~ former stage of ~~said~~ each integration circuit, respectively, and

wherein the physical random number generator includes a polarity switching circuit ~~is provided~~ for switching a ~~the~~ polarity of an input to ~~for said~~ the first selector, ~~said~~ the second selector and ~~said~~ the third selector by ~~the~~ a most significant bit of ~~said~~ the up/down counter.

**Claim 16 (Currently Amended)** A physical random number generator comprising:

one integration circuit for integrating a clock signal through a resistor and a capacitor to output an integral waveform[[,]];

two noise sources[[,]];

two amplifiers, each amplifier for amplifying ~~the~~ a noise ~~of said~~ from a respective noise source of the two noise sources, to output a respective noise signal[[,]];

two mixers, each mixer for mixing ~~said~~ the integral waveform and ~~said~~ a respective noise signal, ~~and~~;

two edge detection circuits, each edge detection circuit for detecting ~~the~~ a first edge of jitter generated based on an output waveform of ~~said~~ a respective mixer of the two mixers; and

a flip-flop for outputting "0" or "1" based on a phase difference ~~in~~ between respective

output signals output from the two ~~output signal between said~~ edge detection circuits;

wherein a variable delay ~~composed of,~~ including a delay and a selector, ~~to adjust~~ for adjusting a ~~the~~ phase of an input signal input into ~~said~~ the flip-flop is provided at ~~the~~ a former or latter stage of ~~said~~ each edge detection circuit, and

wherein the physical random number generator includes a feedback circuit for feeding back the output of ~~said~~ the flip-flop to ~~said~~ the variable delay so that the "0" or the "1" output from ~~said~~ the flip-flop ~~may converge~~ converges to 50%.

**Claim 17 (Currently Amended)** The physical random number generator according to claim 15, wherein ~~an~~ a FET (Field Effect Transistor) is additionally provided in parallel to the capacitor of ~~said~~ each integration circuit at ~~the~~ a latter stage of the resistor of ~~said~~ each integration circuit.

**Claim 18 (Currently Amended)** A ~~The~~ physical random number generator comprising:

two integration circuits, each integration circuit for integrating a clock signal using ~~according to claim 15, wherein~~ a constant current circuit ~~is provided instead of the resistor in said integration circuit~~ and a capacitor to output a respective integral waveform;

two noise sources;

two amplifiers, each amplifier for amplifying a noise from a respective noise source of the two noise sources, to output a respective noise signal;

two mixers, each mixer for mixing a respective integral waveform and a respective noise signal;

two edge detection circuits, each edge detection circuit for detecting a first edge of jitter generated based on an output waveform of a respective mixer of the two mixers;

a flip-flop for outputting "0" or "1" based on a phase difference between respective output signals output from the two edge detection circuits;

a phase adjuster for adjusting a phase of an input signal input into each integration circuit, the phase adjuster including a delay, a first selector and an up/down counter; and

a feedback circuit for feeding back the output of the flip-flop to the phase adjuster so that the "0" or the "1" output from the flip-flop converges to 50%;

wherein a second selector and a third selector are provided at a former stage of each integration circuit, respectively, and

wherein the physical random number generator includes a polarity switching circuit for switching a polarity of an input to the first selector, the second selector and the third selector by a most significant bit of the up/down counter.

**Claim 19 (Currently Amended)** A physical random number generation device wherein two or more physical random number generators according to claim 15 are connected in parallel, ~~and~~ such that ~~the parallel~~ physical random numbers input into ~~said~~ each physical random number generator are input to each physical random number generator in parallel and are rearranged by the physical random number generators into ~~the~~ serial physical random numbers that are ~~then~~ output from the physical random number generators in serial form.

**Claim 20 (Currently Amended)** The physical random number generator according to claim

16, wherein ~~an~~ a FET (Field Effect Transistor) is additionally provided in parallel to the capacitor of ~~said~~ each integration circuit at ~~the~~ a latter stage of the resistor of ~~said~~ each integration circuit.

**Claim 21 (Currently Amended)** A ~~The~~ physical random number generator comprising:

one integration circuit for integrating a clock signal ~~according to claim 16, wherein~~ using a constant current circuit ~~is provided instead of the resistor in said integration circuit~~ and a capacitor to output an integral waveform;

two noise sources;

two amplifiers, each amplifier for amplifying a noise from a respective noise source of the two noise sources, to output a respective noise signal;

two mixers, each mixer for mixing the integral waveform and a respective noise signal;

two edge detection circuits, each edge detection circuit for detecting a first edge of jitter generated based on an output waveform of a respective mixer of the two mixers; and

a flip-flop for outputting "0" or "1" based on a phase difference between respective output signals output from the two edge detection circuits;

wherein a variable delay, including a delay and a selector, for adjusting a phase of an input signal input into the flip-flop is provided at a former or latter stage of each edge detection circuit, and

wherein the physical random number generator includes a feedback circuit for feeding back the output of the flip-flop to the variable delay so that the "0" or the "1" output from the flip-flop converges to 50%.

**Claim 22 (Currently Amended)** A physical random number generation device wherein two or more physical random number generators according to claim 16 are connected in parallel, ~~and~~ such that the ~~parallel~~ physical random numbers input into ~~said~~ each physical random number generator are input to each physical random number generator in parallel and are rearranged by the physical random number generators into ~~the~~ serial physical random numbers that are ~~then~~ output from the physical random number generators in serial form.